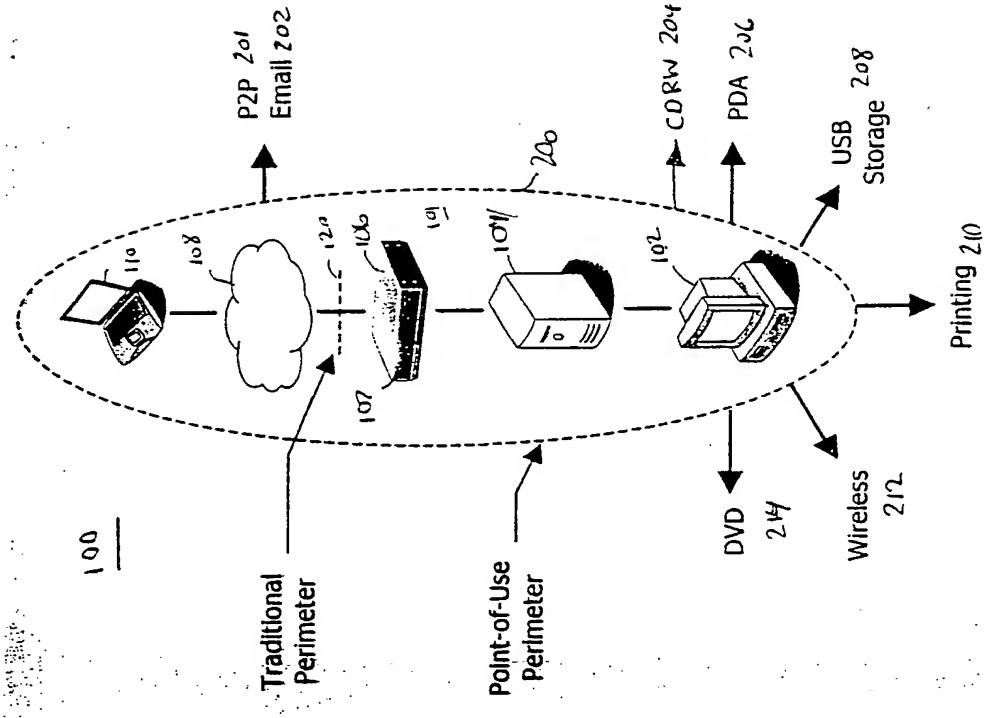
P2P 201
Email 202
CDRW 204
PDA 206
USB Storage 208
Printing 210
DVD 214
Wireless 212
Traditional Perimeter
Point-of-Use Perimeter
100
110
108
120
105
101
107
103
102
200

Fig. 1

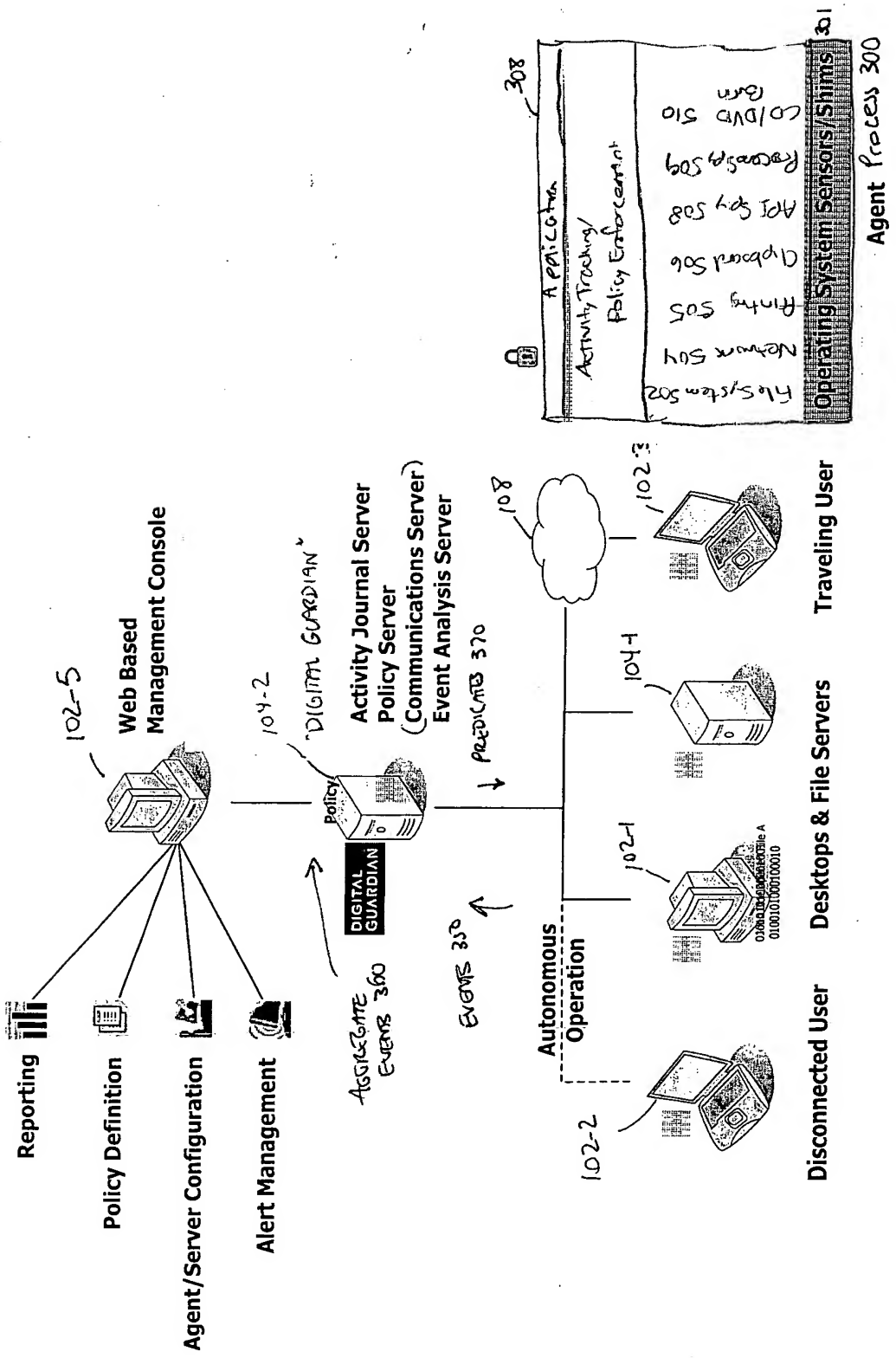
Reporting
Policy Definition
Agent/Server Configuration
Alert Management
Web Based Management Console
102-5
Activity Journal Server
Policy Server
(Communications Server)
Event Analysis Server
104-2
DIGITAL GUARDIAN
Policy
DIGITAL GUARDIAN
Aggregate Events 360
Events 350
Policies 370
108
Autonomous Operation
102-1
102-2
102-3
104-1
Disconnected User
Desktops & File Servers
Traveling User
Agent Process 300
Operating System Sensors/Shims
301
308
Application
Activity Tracking/
Policy Enforcement
File System 502
Network 504
Printing 505
Clipboard 506
API Spy 508
Keystroke 509
CD/DVD 510
Other

Fig. 2

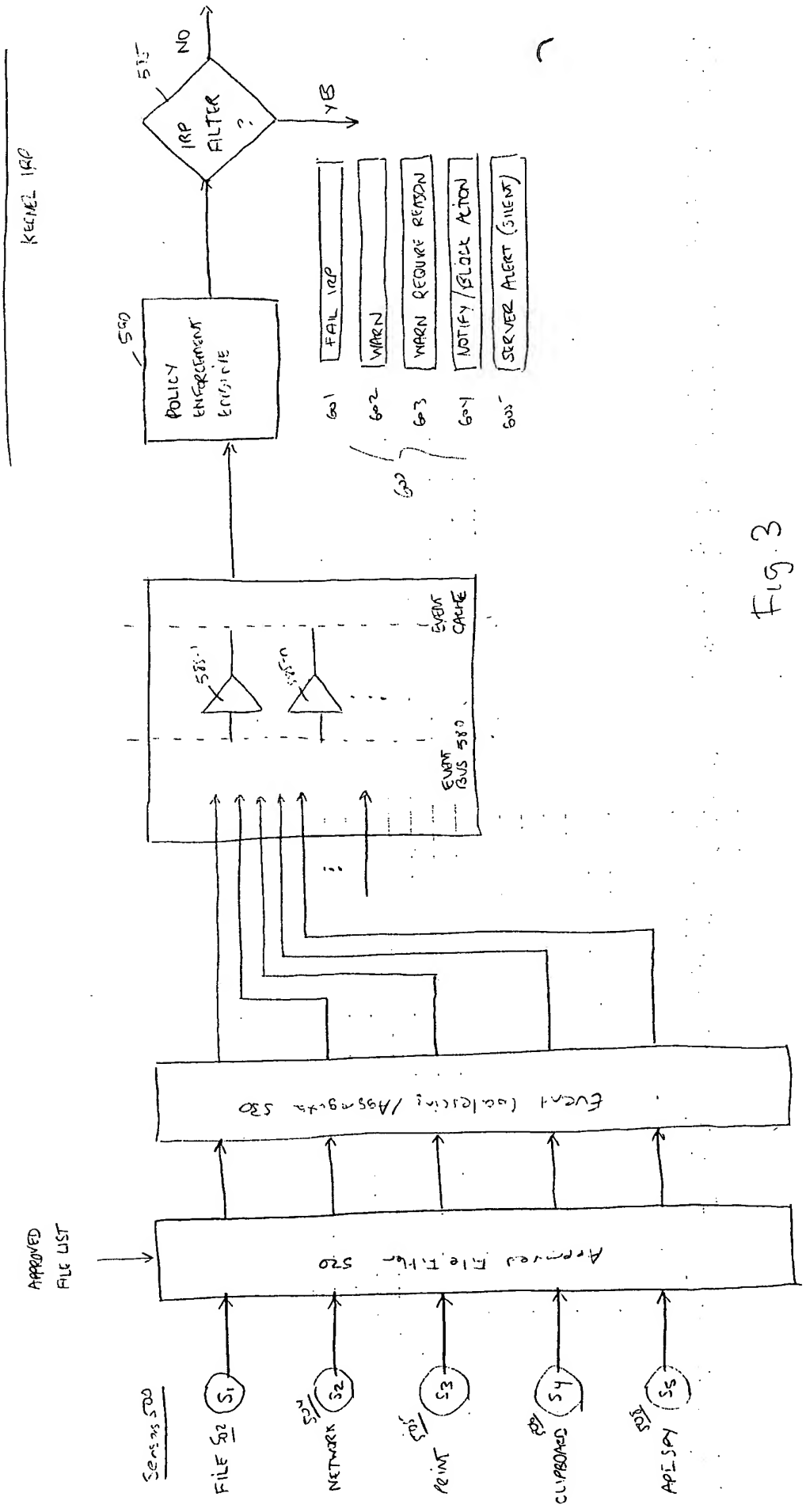
KERNEL IRP
IRP FILTER ?
NO
YES
POLICY ENFORCEMENT ENGINE
FAIL IRP
WARN
WARN REQUIRE REASON
NOTIFY/BLOCK ACTION
SERVER ALERT (SILENT)
EVENT CACHE
EVENT BUS
APPROVED FILE LIST
Approved File Filter
Event Logging/Assembly
FILE
NETWORK
PRINT
CLIPBOARD
API SPY
Sensors

Fig. 3

Atomic Events

| Action ID | Event Level | Event Category | Event | Event Table | Action Detail Field | Action Detail Value | Action Detail Discriminator |
|---|---|---|---|---|---|---|---|
| 1 | Low | File | FileRead | FileEvent | operationType | 0 | bytesRead > 0, bytesWritten = 0 |
| 2 | Low | File | FileWrite | FileEvent | operationType | 0 | bytesRead = 0, bytesWritten > 0 |
| 3 | Low | File | FileReadWrite | FileEvent | operationType | 0 | bytesRead > 0, bytesWritten > 0 |
| 4 | Low | File | FileCopy | FileEvent | operationType | 1 | |
| 5 | Low | File | FileRename | FileEvent | operationType | 2 | |
| 6 | Low | File | FileDelete | FileEvent | operationType | 3 | |
| 7 | Low | File | FileMove | FileEvent | operationType | 4 | |
| 8 | Low | File | FileRecycle | FileEvent | operationType | 5 | |
| 9 | Low | File | FileRestore | FileEvent | operationType | 6 | |
| 10 | Low | Network | TCPIPInbound | NetworkEvent | protocolType | TCPIP | isOutbound = 0 |
| 11 | Low | Network | TCPIPOutbound | NetworkEvent | protocolType | TCPIP | isOutbound = 1 |
| 12 | Low | Network | UDPInbound | NetworkEvent | protocolType | UDP | isOutbound = 0 |
| 13 | Low | Network | UDPOutbound | NetworkEvent | protocolType | UDP | isOutbound = 1 |
| 14 | Low | Network | IPSECInbound | NetworkEvent | protocolType | IPSEC | isOutbound = 0 |
| 15 | Low | Network | IPSECOutbound | NetworkEvent | protocolType | IPSEC | isOutbound = 1 |
| 16 | Low | Print | Print | PrintEvent | (Implied) | N/A | |
| 17 | Low | CD | CDRead | CDEvent | operationType | 1 | |
| 18 | Low | CD | CDWrite | CDEvent | operationType | 2 | |
| 19 | Low | Clipboard | ClipboardCutCopy | ClipboardEvent | eventType | CutCopy | |
| 20 | Low | Clipboard | ClipboardPaste | ClipboardEvent | eventType | Paste | |
| 21 | Low | User | UserLogon | UserEvent | eventType | Logon | |
| 22 | Low | User | UserLogoff | UserEvent | eventType | Logoff | |
| 23 | Low | Machine | Machine | MachineEvent | eventType | ... | Skip the Machine events. |
| 24 | Low | Process | ProcessStart | Process | (Implied) | | Use processStartDtTm |
| 25 | Low | Process | ProcessEnd | Process | (Implied) | | Use processEndDtTime |
| 26 | High | File | FileEdited | AggregateEvent | | | |
| 27 | High | File | FileCopied | AggregateEvent | | | |
| 28 | High | File | FileSaveAs | AggregateEvent | | | |
| 29 | High | File | FileLeftThroughRemovableMedia | AggregateEvent | | | |
| 30 | High | Clipboard | ClipboardToFile | AggregateEvent | | | |
| 31 | High | Print | PrintFile | AggregateEvent | | | |
| 32 | High | CD | BurnMaster | AggregateEvent | | | |
| 33 | High | CD | BurnFile | AggregateEvent | | | |
| 34 | High | Network | FileLeftThroughNetworkPort | AggregateEvent | | | |
| 35 | High | Network | EmailFile | AggregateEvent | | | |
| 36 | High | Network | RemoteAccess | AggregateEvent | | | |
| 37 | High | Network | InstantMessenger | AggregateEvent | | | |
| 38 | High | Network | P2PApp | AggregateEvent | | | |
| 39 | High | Network | FTPFile | AggregateEvent | | | |
| 40 | High | Network | TunnelOut | AggregateEvent | | | |
| 41 | High | Network | TunnelIn | AggregateEvent | | | |
| 42 | High | Network | TunnelInOut | AggregateEvent | | | |
| 43 | High | Network | FileOutThroughTunnel | AggregateEvent | | | |

FIG. 4

Aggregate Event Definitions

| Event Name | Constituent Event Types | Pattern | Scope |
|---|---|---|---|
| FileEdited | FileRead, FileWrite, FileReadWrite | Same processId and fileHandle.<br>beforeHash of first read & afterHash of last write differ.<br>Both reads and writes to same fileHandle.<br>Sum of writes > 0. | Thread |
| FileCopied | FileRead, FileWrite, FileReadWrite, FileCopy | Command shell: Alternating reads & writes. The reads all have one filehandle, the writes all have a second one.<br><br>Explorer: A long series of reads from one filehandle followed by a long series of writes to a second. Mind the time period between.<br><br>In both cases, the target device must not be removable. | Thread |
| FileSaveAs | FileRead, FileWrite, FileReadWrite | An app reads one or more files then writes a file | Process |
| FileLeftThroughRemovableMedia | FileRead, FileWrite, FileReadWrite, FileCopy | Same as FileCopied or FileSaveAs, but target device is removable. | Process |
| ClipboardToFile | ClipboardCutCopy, ClipboardPaste | Pair a ClipboardCutCopy with all subsequent ClipboardPaste events for that user login until the next copy or the user logs out.<br><br>Problem: If the user closes the application that performed the copy and the object was large and the user opts not to keep it there, what happens? | Login |
| PrintFile | Print, possibly others | Unclear. If there are temp files, intermediate PDF files, etc, then we may perform a chain of custody analysis to figure out just what was printed. | Thread |
| BurnMaster | FileRead, FileWrite | An app known to burn files reads one or more files then writes a file. | Process |
| BurnFile | CDWrite, FileRead | Application is recognized as a CD writing app. (Optional)<br><br>Series of FileReads from one fileHandle, followed by a series of CDWrite events with the same process. May need to compare filenames, otherwise one read will exhaust all the writes. Alternately, all read files are lumped together with one large burn event. Or perhaps the first read of a new file after the last read from the previous file is the start of the next burn event. | Process |
| FileLeftThroughNetworkPort | FileRead,<br>TCPIPInbound, TCPIPOutbound,<br>UDPInbound, UDPOutbound,<br>IPSECInbound, IPSECOutbound | An overlapping stream of FileReads interspersed with Inbound and Outbound network events.<br><br>All the network events should be for the same port (?) and to a destination NOT on localhost.<br><br>All the network events should be for the same protocol. | Thread |

Fig. 5A

Aggregate Event Definitions

| Event Name | Constituent Event Types | Pattern | Scope |
|---|---|---|---|
| EmailFile | FileRead, TCPIPInbound, TCPIPOutbound, (other protocols???) | Similar to FileLeftThroughNetworkPort. Combines all interleaving FileReads with the network events.<br><br>The application image name is one of those known to be an email program.<br><br>May place constraints on the ports, since many emailers use certain well defined ports for SMTP, POP etc. | Process |
| InstantMessenger | FileRead, TCPIPInbound, TCPIPOutbound, (other protocols???) | Similar to FileLeftThroughNetworkPort. Combines all interleaving FileReads with the network events.<br><br>The application image name is one of those known to be used for Instant Messenger.<br><br>May place constraints on the ports. | Process |
| P2PApp | FileRead, TCPIPInbound, TCPIPOutbound, UDPInbound, UDPOutbound, IPSECInbound, IPSECOutbound | Constrain the application name to be one of those known to be a P2PApp.<br><br>Multiple ports will be used; some or all of them may have constraints.<br>May constrain the protocol per app or per instance.<br><br>Similar to FileLeftThroughNetworkPort as concerns interleaved file reads. | Process |
| FTPFile | FileRead, FileWrite, ??? (TCPIPInbound, TCPIPOutbound) | May want to split into two events, one for reading and one for writing.<br><br>Constrain to the common FTP port, unless the app is known by name to be an FTP client.<br><br>Like FileLeftThroughNetworkPort, look for interleaved reads and network events, or interleaved writes and network events. | Process |
| RemoteAccess | TCPIPInbound, TCPIPOutbound, UDPInbound, UDPOutbound, IPSECInbound, IPSECOutbound | Do not incorporate FileRead events.<br><br>Several ports may be used.<br><br>Look for known image names of remote apps. | Process |
| TunnelOut | TCPIPInbound, TCPIPOutbound, UDPInbound, UDPOutbound, IPSECInbound, IPSECOutbound | All events use same protocol. Only two processes used.<br>Two different apps and four ports are used. One of the ports is remote.<br>Event 1: The first app sends outbound from local port 1 to local port 2.<br>Event 2: The second app (the tunneler) receives inbound from local port 1 to local port 2.<br>Event 3: The tunneler also sends from local port 3 to remote port 4.<br>Both events of the tunneler share the same thread (probably). | Login |
| TunnelIn | TCPIPInbound, TCPIPOutbound, UDPInbound, UDPOutbound, IPSECInbound, IPSECOutbound | All events use same protocol. Only two processes used.<br>Two different apps and four ports are used. One of the ports is remote.<br>Event 1: The first app (the tunneler) receives inbound from remote port 1 to local port 2.<br>Event 2: The tunneler sends outbound from local port 2 to local port 3.<br>Event 3: The second app also receives inbound from local port 3 to local port 4.<br>Both events of the tunneler share the same thread (probably). | Login |
| TunnelInOut | TCPIPInbound, TCPIPOutbound, UDPInbound, UDPOutbound, IPSECInbound, IPSECOutbound | Multiple protocols may be used. More research needed. More than three ports are used. | Login |

FIG. 5B

Aggregate Event Definitions

| Event Name | Constituent Event Types | Pattern | Scope |
|---|---|---|---|
| FileLeftThroughTunnel | FileRead, TunnelOut | Similar to FileLeftThroughNetworkPort. Combines all interleaving FileReads involving a process that is participating in a TunnelOut event.<br><br>If more than one file is read, the source destination will be a count of the files read. | Login? |

FIG. 5C

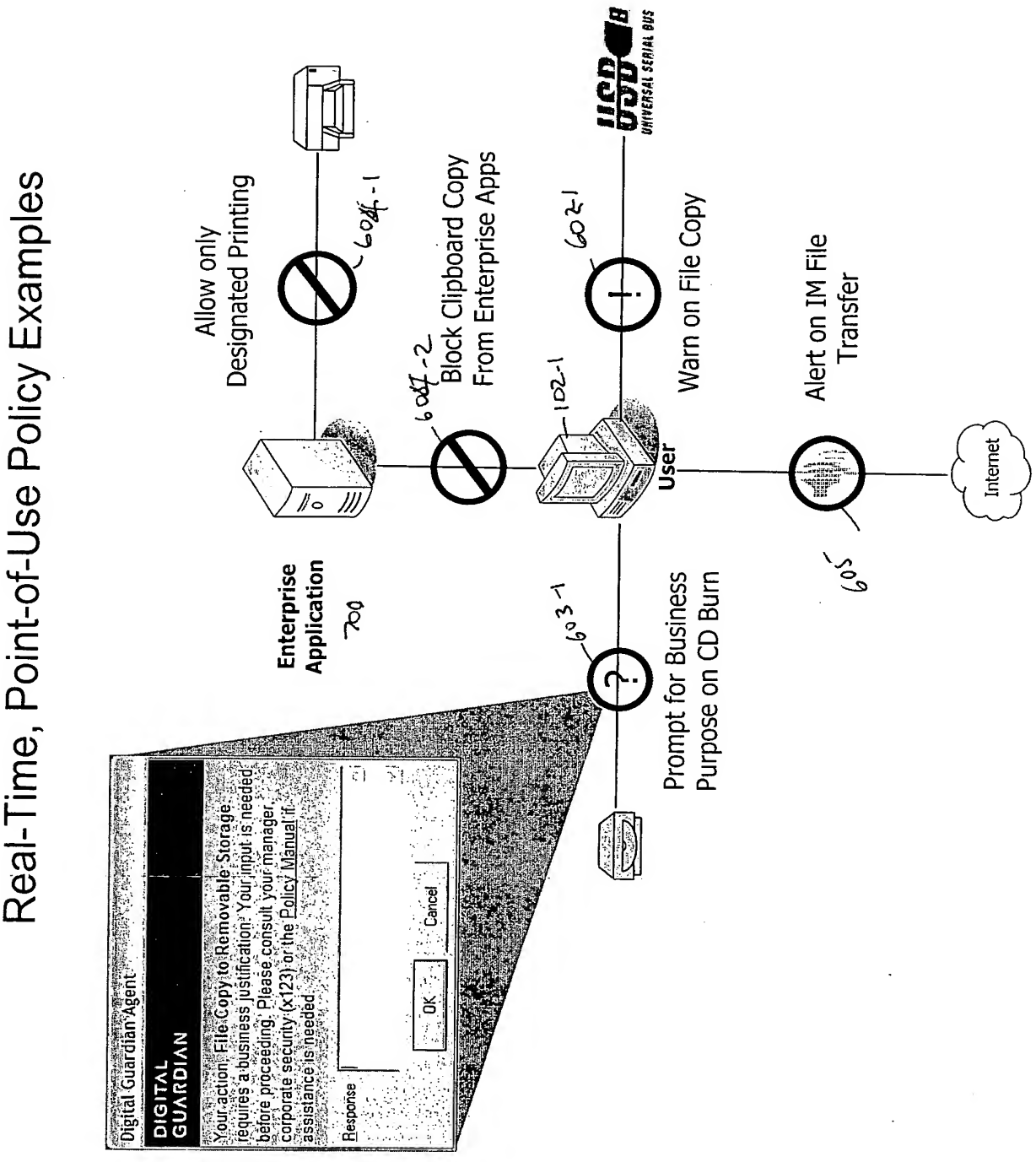
Real-Time, Point-of-Use Policy Examples
Allow only Designated Printing
604-1
Block Clipboard Copy From Enterprise Apps
604-2
Warn on File Copy
602-1
Alert on IM File Transfer
605
Prompt for Business Purpose on CD Burn
603-1
Enterprise Application
700
User
102-1
Internet
USB
UNIVERSAL SERIAL BUS
Digital Guardian Agent
DIGITAL GUARDIAN
Your action: File Copy to Removable Storage requires a business justification. Your input is needed before proceeding. Please consult your manager, corporate security (x123) or the Policy Manual if assistance is needed.
Response
OK
Cancel

Fig. 6